On the genericity of pseudo-Anosov braids II: conjugations to rigid braids

Sandrine Caruso, Bert Wiest

ON THE GENERICITY OF PSEUDO-ANOSOV BRAIDS II: CONJUGATIONS TO RIGID BRAIDS

SANDRINE CARUSO AND BERT WIEST

ABSTRACT. We prove that generic elements of braid groups are pseudo-Anosov, in the following sense: in the Cayley graph of the braid group with $n \geqslant 3$ strands, with respect to Garside's generating set, we prove that the proportion of pseudo-Anosov braids in the ball of radius l tends to 1 exponentially quickly as l tends to infinity. Moreover, with a similar notion of genericity, we prove that for generic pairs of elements of the braid group, the conjugacy search problem can be solved in quadratic time. The idea behind both results is that generic braids can be conjugated "easily" into a rigid braid.

1. INTRODUCTION

In the recent article [1], S. Caruso proved the following result. For a fixed number of strands n, consider the ball of radius l and center 1 in the Cayley graph of the braid group $\mathcal{B}_n$, with generators the simple braids. Then for sufficiently large l, among the elements of this ball, the proportion of pseudo-Anosov braids is bounded below by a positive constant which does not depend on l (but it might depend on n). A key lemma in this paper states that among the *rigid* braids with canonical length equal to l, the proportion of pseudo-Anosov braids tends to 1 as l tends to infinity.

The aim of the present paper is to prove the following stronger result:

Theorem 5.1. *Consider the ball of radius l and center 1 in the Cayley graph of the braid group $\mathcal{B}_n$, with generators the simple braids. Then the proportion of pseudo-Anosov braids among the elements of this ball tends to 1 as l tends to infinity. Moreover, this convergence happens exponentially fast.*

In fact, we shall prove a slightly stronger technical result: in the statement of the theorem, one can replace "pseudo-Anosov braids" by "braids which admit a non-intrusive conjugation to a rigid pseudo-Anosov braid".

The plan of the article is as follows: in Section 2, we recall some classical definitions. In Section 3, we state the fact that, among braids with a fixed infimum, the proportion of those admitting a non-intrusive conjugation to a rigid braids tends to 1 exponentially quickly as the canonical length tends to infinity. This fact will be proven in Section 4, using the notion of a blocking braid. We complete the proof of the main theorem in Section 5. In Section 6 we prove a related result, namely that the conjugacy problem in braid groups has generically a fast solution. Finally, we present some other consequences and conjectures arising from our results and techniques in Section 7.

2. DEFINITIONS

We recall that the Nielsen-Thurston classification theorem states that every element of B_n is exactly one of the following: periodic, or reducible non-periodic, or pseudo-Anosov. In the context of braid groups, we must use the following definition of *periodic*: a braid $x \in \mathcal{B}_n$ is periodic if and only if there exist non-zero integers m and l such that $x^m = \Delta^l$, where $\Delta = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1$. (Geometrically, Δ corresponds to a half-twist along the boundary of the disk. The center of $\mathcal{B}_n$ is generated by the full twist Δ^2.)

We will also use some elements of Garside theory, in the classical case of braid groups, which we recall now. For more details, the reader can consult [6], or [4] for the general theory.

The group $\mathcal{B}_n$ is equipped with a partial order relation $\preccurlyeq$, defined as follows: $x \preccurlyeq y$ if and only if $x^{-1}y \in \mathcal{B}_n^+$, the monoid of positive braids (i.e. only positive crossings). If $x \preccurlyeq y$, we say that x is a *prefix* of y. Any two elements $x, y \in \mathcal{B}_n$ have a unique greatest common prefix, denoted $x \wedge y$.

Similarly we define $\succcurlyeq$ as follows: $x \succcurlyeq y$ if and only if $xy^{-1} \in \mathcal{B}_n^+$. Notice that $x \succcurlyeq y$ is not equivalent to $y \preccurlyeq x$. If $x \succcurlyeq y$, we say that y is a *suffix* of x.

The elements of the set $\{x \in \mathcal{B}_n, 1 \preccurlyeq x \preccurlyeq \Delta\}$ are called *simple braids*, or *permutation braids*. Throughout this paper, we shall use the set of simple braids as the generating set of $\mathcal{B}_n$. The ball of radius l and center 1 in the Cayley graph of $\mathcal{B}_n$ with respect to this generating set will be denoted $\mathbf{B}(l)$.

Definition 2.1 (left-weighting)**.** Let s_1, s_2 be two simple braids in $\mathcal{B}_n$. We say that s_1 and s_2 are *left-weighted*, or that the pair (s_1, s_2) is left-weighted, if there does not exist any generator σ_i such that $s_1\sigma_i$ and $\sigma_i^{-1}s_2$ are both still simple.

Definition 2.2 (starting set, finishing set)**.** Let $s \in \mathcal{B}_n$ be a simple braid. We call *starting set of* s the set $S(s) = \{i,\ \sigma_i \preccurlyeq s\}$ and *finishing set of* s the set $F(s) = \{i,\ s \succcurlyeq \sigma_i\}$.

Remark 2.3. Two simple braids s_1 and s_2 are left-weighted if and only if $S(s_2) \subset F(s_1)$.

Proposition 2.4. *Let $x \in \mathcal{B}_n$. There exists a unique decomposition $x = \Delta^p x_1 \cdots x_r$ such that $x_1, \ldots, x_r$ are simple braids, distinct from Δ and 1, and such that the pairs (x_i, x_{i+1}) are left-weighted for all $i = 1, \ldots, r-1$.*

Definition 2.5 (left normal form)**.** In the previous proposition, the writing $x = \Delta^p x_1 \cdots x_r$ is called the *left normal form* of x, p is called the *infimum* of x and is denoted by $\inf(x)$, $p+r$ is the *supremum* of x and is denoted by $\sup(x)$, and r is called the *canonical length* of x, and denoted $\ell_c(x)$.

Furthermore, if $r \geqslant 1$, we denote by $\iota(x) = \tau^{-p}(x_1)$ the *initial factor* of x, where τ denotes the conjugation by Δ, i.e. $\tau(x) = \Delta^{-1}x\Delta$. (In particular $\iota(x) = x_1$ if p is even, $\iota(x) = \Delta x_1 \Delta^{-1}$ if p is odd.) We denote $\varphi(x) = x_r$ the *final factor* of x.

Definition 2.6 (rigidity)**.** A braid x of positive canonical length is said to be *rigid* if the pair $(\varphi(x), \iota(x))$ is left-weighted.

Finally, we mention that at several key points in the present paper we shall use the article [1], and particularly its asymptotic estimates. For two number sequences (u_l) and (v_l), we say that u_l is of the order of v_l if the sequences $(\frac{u_l}{v_l})$ and $(\frac{v_l}{u_l})$ are bounded.

3. NON-INTRUSIVE CONJUGATIONS

Definition 3.1. Let x be a braid with normal form $x = \Delta^{\inf(x)} x_1 \cdot \cdots \cdot x_l$. A conjugation of x is *non-intrusive* if the normal form of the conjugated braid contains the subword $x_{2\cdot\lceil \frac{l}{5}\rceil+1} \cdots x_{l-2\cdot\lceil \frac{l}{5}\rceil}$.

In other words, a conjugation of x is non-intrusive if the middle fifth of the normal form of x still appears in the normal form of the conjugate.

Example 3.2. Let x be the following braid with 4 strands and of canonical length 5:

$$x = \sigma_2\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2 \cdot \sigma_3\sigma_2\sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1.$$

Its middle fifth consists of the single factor $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$. Let $\tilde{x}$ be its conjugate by the last two factors $\sigma_3\sigma_2\sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1$:

$$\begin{aligned}\tilde{x} &= \sigma_3\sigma_2\sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_2\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2 \\ &= \Delta \cdot \sigma_1\sigma_2\sigma_3\sigma_1 \cdot \sigma_1\sigma_3 \cdot \sigma_1\sigma_3\sigma_2\sigma_1 \cdot \sigma_1\sigma_2\sigma_1\sigma_3\sigma_2 \quad \text{(in normal form)}\end{aligned}$$

The conjugation from x to $\tilde{x}$ is non intrusive, because $\tilde{x}$ contains the factor $\sigma_1\sigma_2\sigma_1\sigma_3\sigma_2$ in its normal form.

Notation 3.3. We denote

$$\mathcal{B}_n^{\epsilon,l} = \{x \in \mathcal{B}_n \mid \inf(x) = \epsilon, \ell_c(x) = l\}$$

and $\rho_n^{(\epsilon,l)}$ the proportion, among the elements of $\mathcal{B}_n^{\epsilon,l}$, of braids which admit a non-intrusive conjugation to a rigid braid.

We observe that for every $l \in \mathbb{N}$ and $\epsilon \in \mathbb{Z}$ we have $\rho_n^{(\epsilon,l)} = \rho_n^{(\epsilon+2,l)}$ – thus $\rho_n^{(\epsilon,l)}$ depends only on n, on l, and on the parity of ϵ.

Proposition 3.4. *There exists a constant $\mu_R \in (0,1)$ (which depends on n) such that $\rho_n^{(\epsilon,l)} \geqslant 1-\mu_R^l$.*

The aim of the next section is to prove this proposition.

4. BLOCKING BRAIDS AND THE PROOF OF PROPOSITION 3.4

Notation 4.1. If X and Y are two braids, and if Y is of infimum 0, then we denote $\mathrm{NF}_l(X \cdot Y)$ the word in (left) normal form representing the product $X \cdot Y$.

We say that $X \cdot Y$ *is in normal form* if $\mathrm{NF}_l(X \cdot Y)$ is equal, as a word, to the normal form of X, followed by the normal form of Y.

If s_1 is the last factor of the normal form of X, and s_2 is the first factor of the normal form of Y, we are going to denote $F(X) = F(s_1)$ and $S(Y) = S(s_2)$. In particular, $X \cdot Y$ is in normal form if and only if $S(Y) \subset F(X)$.

Let x be a braid of infimum $\epsilon \in \mathbb{Z}$, and of canonical length $l \geqslant 5$. We introduce some more notation. We cut the normal form representative of x (other than the initial power of Δ) into five

pieces of roughly equal size, each of them in normal form:

$$P_1(x) = x_1 \cdots x_{\lceil \frac{l}{5} \rceil}, \quad P_2(x) = x_{\lceil \frac{l}{5} \rceil + 1} \cdots x_{2 \cdot \lceil \frac{l}{5} \rceil},$$
$$P_3(x) = x_{2 \cdot \lceil \frac{l}{5} \rceil + 1} \cdots x_{l - 2 \cdot \lceil \frac{l}{5} \rceil},$$
$$P'_4(x) = x_{l - 2 \cdot \lceil \frac{l}{5} \rceil + 1} \cdots x_{l - \lceil \frac{l}{5} \rceil}, \quad P'_5(x) = x_{l - \lceil \frac{l}{5} \rceil + 1} \cdots x_l.$$

Notice that $P_1(x), P_2(x), P'_4(x)$ and $P'_5(x)$ have exactly equal length. The word $P_3(x)$ is the "middle fifth" subword mentioned in the previous section. Finally, we denote

$$P_4(x) = \tau^{\epsilon}(P'_4(x)) \text{ et } P_5(x) = \tau^{\varepsilon}(P'_5(x)).$$

If there is no ambiguity, we shall simply write P_i instead of $P_i(x)$. The braid x can always be conjugated to

$$\tilde{x} = \Delta^{\epsilon} \cdot P_4 \cdot P_5 \cdot P_1 \cdot P_2 \cdot P_3$$

and this writing is almost in normal form: the only place where two successive letters are not necessarily left-weighted is the transition from the last letter of P_5 to the first letter of P_1. All other pairs of successive letters are left-weighted, even $\varphi(P_3)$ followed by $\iota(\Delta^{\varepsilon} P_4)$ (the last letter followed by the first). For this reason we also have $\iota(P_4) = \iota(P_4 \cdot P_5)$ and $\varphi(P_1 \cdot P_2) = \varphi(P_2)$.

Observation 4.2. Consider the normal form of $P_4 \cdot P_5 \cdot P_1 \cdot P_2$. If

$$\iota(P_4 \cdot P_5 \cdot P_1 \cdot P_2) = \iota(P_4 \cdot P_5) \tag{1}$$

and

$$\varphi(P_4 \cdot P_5 \cdot P_1 \cdot P_2) = \varphi(P_1 \cdot P_2) \tag{2}$$

then the braid $\tilde{x}$ is non-intrusively conjugate to x (because the normal form of $\tilde{x}$ will contain P_3 as a subword), and it is rigid.

Intuitively, the hypothesis of Observation 4.2 is that the given word representing $\tilde{x}$ may not quite be in normal form, but that the modifications necessary in order to transform it into normal form are confined inside the word, and do not touch its extremities (up to a possible appearance of some factors Δ, and up to conjugation of the initial factors of $\tilde{x}$ by these factors Δ.)

For instance, in Example 3.2, the hypotheses of Observation 4.2 are satisfied, and the conjugate $\tilde{x}$ is indeed rigid.

Our aim now is to prove that the proportion of braids x for which the hypotheses of Observation 4.2 are satisfied tends to 1 when the length of x tends to infinity. In order to achieve this, we are going to observe that certain braids "block the chain reaction of the transformation into normal form", and that these "blocking braids" have excellent chances of actually appearing.

We recall that for a simple braid s, the *complement* ∂s is the braid $\partial s = s^{-1}\Delta$. We extend this definition to arbitrary braids y by the formula

$$\partial y = y^{-1} \cdot \Delta^{\sup(y)}.$$

This is the unique braid such that $y \cdot \partial y = \Delta^{\sup(y)}$. If the normal form of y is $\Delta^{\inf y} y_1 \cdots y_l$ then the normal form of ∂y is $\bar{y}_l \cdots \bar{y}_1$, where $\bar{y}_{l-i} = \tau^{-i}(\partial y_{l-i})$ for $i = 0, \ldots, l-1$ (i.e. $\bar{y}_{l-i} = y_{l-i}^{-1} \cdot \Delta =$

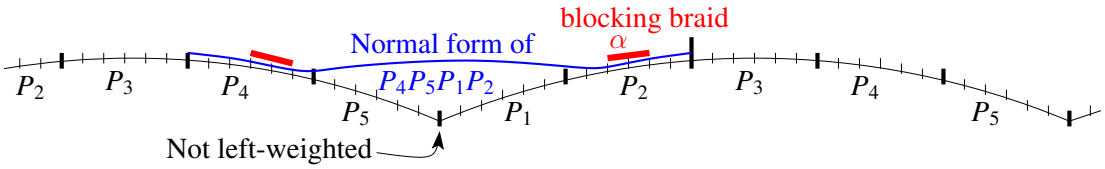

FIGURE 1. The stategy of the proof: this picture takes place in the Cayley graph of $\mathcal{B}_n$. The braid x lifts to a bi-infinite path. The picture shows the generic situation: the last factor of the normal form of $P_4P_5P_1P_2$ coincides with the last factor of P_2, and its initial factor (except for Δ) coincides with the first factor of P_4.

∂y_{l-i} if i is even and $\bar{y}_{l-i} = \Delta \cdot y_{l-i}^{-1} = \tau^{-1}(\partial y_{l-i})$ if i is odd). In particular, $\inf(\partial y) = 0$ and $\sup(\partial y) = \ell_c(y)$. We also calculate, for later reference, that

$$\varphi(\partial y) = \tau^{-\sup(y)+1}(\partial\iota(y)) \tag{3}$$

because $\varphi(\partial y) = \bar{y}_1 = \tau^{-l+1}(\partial y_1) = \tau^{-l+1}(\partial\tau^{-\inf(y)}\iota(y)) = \tau^{-\inf(y)-l+1}(\partial\iota(y))$.

Now, the normal form representative of $P_4 \cdot P_5 \cdot P_1 \cdot P_2$ is

$$\mathrm{NF}_l\left(P_4 \cdot P_5 \cdot P_1 \cdot P_2\right) = \mathrm{NF}_l\left(P_4 \cdot P_5 \cdot t\right) \cdot \mathrm{NF}_l\left(t^{-1} \cdot P_1 \cdot P_2\right) \tag{4}$$

where

$$t = (P_1 \cdot P_2) \wedge \partial(P_4 \cdot P_5).$$

We also notice that, since $P_4 \cdot P_5 \cdot t \cdot t^{-1} \cdot \partial(P_4 \cdot P_5) = \Delta^{\sup(P_4P_5)} = \Delta^{\sup(P_4P_5t)}$, the following formula holds:

$$\partial(P_4 \cdot P_5 \cdot t) = t^{-1} \cdot \partial(P_4 \cdot P_5). \tag{5}$$

This suggests a way of studying the normal form of $P_4 \cdot P_5 \cdot P_1 \cdot P_2$ in which $P_1 \cdot P_2$ and $\partial(P_4 \cdot P_5)$ play strictly symmetric roles:

Lemma 4.3. *Still denoting $t = (P_1 \cdot P_2) \wedge \partial(P_4 \cdot P_5)$, suppose that*

$$\varphi(t^{-1} \cdot P_1 \cdot P_2) = \varphi(P_1 \cdot P_2), \tag{6}$$

and

$$\varphi(t^{-1} \cdot \partial(P_4 \cdot P_5)) = \varphi(\partial(P_4 \cdot P_5)). \tag{7}$$

Then the hypotheses of Observation 4.2 are satisfied, and the braid x is non-intrusively conjugate to a rigid braid.

Proof. Let us suppose that (6) holds. Then so does (2), because

$$\varphi(P_4 \cdot P_5 \cdot P_1 \cdot P_2) \overset{(4)}{=} \varphi(t^{-1} \cdot P_1 \cdot P_2) \overset{(6)}{=} \varphi(P_1 \cdot P_2)$$

Let us now prove the implication from (7) to (1). Assuming (7), we calculate

$$\tau^{\sup(P_4\cdot P_5\cdot t)-1}(\partial\iota(P_4 \cdot P_5 \cdot t)) \overset{(3)}{=} \varphi(\partial(P_4 \cdot P_5 \cdot t)) = \varphi(t^{-1} \cdot \partial(P_4 \cdot P_5)) \overset{(7)}{=}$$
$$\overset{(7)}{=} \varphi(\partial(P_4 \cdot P_5)) = \tau^{\sup(P_4\cdot P_5)-1}(\partial\iota(P_4 \cdot P_5)).$$

Since $\sup(P_4 \cdot P_5 \cdot t) = \sup(P_4 \cdot P_5)$, this implies $\iota(P_4 \cdot P_5 \cdot t) = \iota(P_4 \cdot P_5)$, i.e. (1). □

Our aim now is to show that, in most cases, (6) and (7) are indeed satisfied.

Definition 4.4. A positive braid α is a *blocking braid* if there exists an $i \in \{1, ..., n-1\}$ so that for each braid X with $\inf(X) = 0$ such that $X \cdot \alpha$ is in left normal form, the only non trivial simple braid which is a suffix of $X \cdot \alpha$ is σ_i. In other words, the last factor of the *right* normal form of $X \cdot \alpha$ must be σ_i.

Lemma 4.5. *Let α be a blocking braid and X be a braid such that* $\inf X = 0$ *and such that $X \cdot \alpha$ is in normal form. Let t be a prefix of $X \cdot \alpha$. If $(\sigma_i =)\varphi(X \cdot \alpha) \neq \varphi(t^{-1} \cdot X \cdot \alpha)$ then $t = X \cdot \alpha$.*

Proof. Let $s = t^{-1} \cdot X \cdot \alpha$ be the braid such that $t \cdot s = X \cdot \alpha$ (of course, $t \cdot s$ is not in normal form as written). Let us suppose (to obtain a contradiction) that s is nontrivial. Then $\varphi(s)$ is a nontrivial simple braid which is a suffix of s and so of $t \cdot s = X \cdot \alpha$. Yet, by hypothesis, the only nontrivial simple braid which is a suffix of $X \cdot \alpha$ is σ_i. So $\varphi(X \cdot \alpha) = \varphi(s)$: contradiction. □

Lemma 4.6. *Let α be a blocking braid and let X, Y be braids such that* $\inf X = \inf Y = 0$ *and such that $X \cdot \alpha \cdot Y$ is in normal form. Let t be a prefix of $X \cdot \alpha \cdot Y$. If $\varphi(t^{-1} \cdot X \cdot \alpha \cdot Y) \neq \varphi(X \cdot \alpha \cdot Y)$, then the normal form of t contains the normal form of $X \cdot \alpha$ as a prefix.*

Proof. Let $t_1 = t \wedge (X \cdot \alpha)$. We claim, and will prove below, that $\varphi(t_1^{-1} \cdot X \cdot \alpha) \neq \varphi(X \cdot \alpha)$. By applying Lemma 4.5 to t_1, we deduce that $X \cdot \alpha$ is a prefix of t. It remains to show that the normal form of $X \cdot \alpha$ is even the beginning of the normal form of t: indeed, t is a prefix of $X \cdot \alpha \cdot Y$ and so $(X \cdot \alpha)^{-1} t$ is a prefix of Y. In particular, $S((X \cdot \alpha)^{-1} t) \subset S(Y) \subset F(\alpha)$, the last inclusion coming from the fact that $X \cdot \alpha \cdot Y$ is in normal form. So $X \cdot \alpha \cdot \mathrm{NF}_l((X \cdot \alpha)^{-1} t)$ is in normal form, which implies what we wanted.

Here is now the proof of our claim. We suppose, for a contradiction, that $\varphi(t_1^{-1} \cdot X \cdot \alpha) = \varphi(X \cdot \alpha)$. This means that $\mathrm{NF}_l(t_1^{-1} \cdot X \cdot \alpha) \cdot Y$ is in normal form. Since $t_1^{-1} t \wedge t_1^{-1} X \cdot \alpha = 1$, we can deduce that we also have $t_1^{-1} t \wedge t_1^{-1} X \cdot \alpha \cdot Y = 1$. Then, as $t_1^{-1} t$ left-divides $t_1^{-1} X \cdot \alpha \cdot Y$, we have $t_1^{-1} t = 1$. Finally, this implies that t is a prefix of $X \cdot \alpha$, and so, by Lemma 4.5, $\varphi(t^{-1} \cdot X \cdot \alpha \cdot Y) = \varphi(X \cdot \alpha \cdot Y)$, contradicting the hypothesis. □

Lemma 4.7. *Blocking braids exist.*

Proof. Here is such a construction: denoting by $\Delta_{i,j}$ the positive half-twist involving the strands $i, i+1, \ldots, j$, let

$$\alpha = \Delta_{1,n-1}\sigma_{n-1} \cdot \Delta_{1,n-2}\sigma_{n-1}\sigma_{n-2} \cdot \Delta_{1,n-3}\sigma_{n-2}\sigma_{n-3} \cdot \Delta_{1,n-4}\sigma_{n-3}\sigma_{n-4} \cdots \sigma_1\sigma_2\sigma_1\sigma_4\sigma_3 \cdot \sigma_1\sigma_3\sigma_2 \cdot \sigma_2.$$

For example with 6 strands (see Figure 2):

$$\alpha = \sigma_1\sigma_2\sigma_3\sigma_4\sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1\sigma_5 \cdot \sigma_1\sigma_2\sigma_3\sigma_1\sigma_2\sigma_1\sigma_5\sigma_4 \cdot \sigma_1\sigma_2\sigma_1\sigma_4\sigma_3 \cdot \sigma_1\sigma_3\sigma_2 \cdot \sigma_2.$$

It is a braid word which is in left normal form, but also in right normal form. We observe that the starting set of α is $S(\alpha) = \{1, ..., n-2\}$ and its finishing set is $F(\alpha) = \{2\}$. If $X \cdot \alpha$ is in (left) normal form, then $F(X) \supseteq \{1, ..., n-2\}$ and so $F(X) = \{1, ..., n-2\}$. This implies that $X \cdot \alpha$ is also in right normal form. So the only simple factor which can be extracted by the right from $X \cdot \alpha$ is σ_2, as we wanted. □

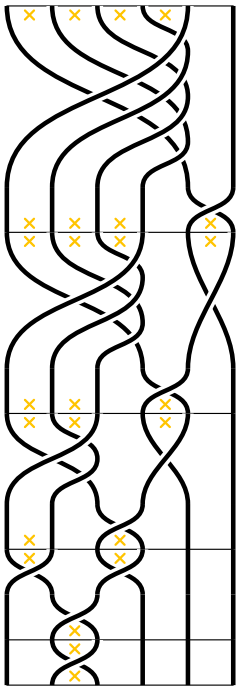

FIGURE 2. Example of a blocking braid with 6 strands. The yellow crosses indicate the starting and finishing sets.

In order to prove that blocking braids are almost certain to occur just where we need them, we will use the following lemma, which results from Lemma 3.5 and Remark 3.6 in [1].

Lemma 4.8. *Let a_1, a_2, $a_3\colon \mathbb{N} \to \mathbb{N}$ be functions with $a_1 + a_3$ and a_2 non-decreasing and tending to infinity, and such that $a_1(l) + a_2(l) + a_3(l) = l$. For each braid x of infimum $\epsilon \in \mathbb{Z}$ and of canonical length l, of normal form $\Delta^\epsilon x_1 \cdots x_l$, denote by $P(x) = x_{a_1(l)+1} \cdots x_{a_1(l)+a_2(l)}$ (so $P(x)$ is a part of the normal form of x of length $a_2(l)$).*

Let w be a fixed braid. Then the proportion of braids $x \in \mathcal{B}_n^{\epsilon,l}$ such that the normal form of $P(x)$ contains that of w as a subword tends exponentially quickly to 1 when l tends to infinity.

Proof of Proposition 3.4. We recall that we have to prove that the proportion, among the braids x in $\mathcal{B}_n^{\epsilon,l}$, of braids for which one of the two hypotheses, (6) or (7), of Lemma 4.3 is *not* satisfied, tends exponentially quickly to 0 as l tends to infinity. In fact, we shall only prove that braids not satisfying hypothesis (6) are rare. Since the operation of taking the complement $\partial\colon \mathcal{B}_n^{0,2\lceil \frac{l}{5} \rceil} \to \mathcal{B}_n^{0,2\lceil \frac{l}{5} \rceil}$ is a bijection, we have a completely analogue situation for hypothesis (7).

By Lemma 4.8, the proportion of braids x such that $P_2(x)$ contains a blocking braid tends to 1 exponentially quickly. Among these braids, look at those for which

$$\varphi(P_4 \cdot P_5 \cdot P_1 \cdot P_2) \neq \varphi(P_1 \cdot P_2)$$

holds, or in other words

$$\varphi(t^{-1}\cdot P_1\cdot P_2)\neq\varphi(P_1\cdot P_2),\quad\text{where}\quad t=(P_1\cdot P_2)\wedge\partial(P_4\cdot P_5)$$

For those braids, by Lemma 4.6, the normal form of t must contain that of P_1 as a prefix, and in particular $P_1\preccurlyeq t$. (Intuitively, the factor P_1 must be completely "eaten" during the transformation of $P_4\cdot P_5\cdot P_1\cdot P_2$ into normal form, possibly creating some new factors Δ.) Thus

$$P_1=P_1\wedge\Delta^{\lceil\frac{l}{5}\rceil}\preccurlyeq t\wedge\Delta^{\lceil\frac{l}{5}\rceil}\preccurlyeq(\partial(P_4\cdot P_5))\wedge\Delta^{\lceil\frac{l}{5}\rceil}=\partial P_5$$

So $P_1(x)$ must be a prefix of $\partial P_5(x)$. Yet, the proportion of braids x for which this is the case is negligible:

Lemma 4.9. *The proportion, among all elements of $\mathcal{B}_n^{\varepsilon,l}$, of braids $x\in\mathcal{B}_n^{\varepsilon,l}$ such that P_1 is a prefix of ∂P_5 decreases exponentially quickly to 0 when l tends to infinity.*

Proof. We decompose ∂P_5 in two parts of length $\lceil\frac{l}{10}\rceil$ and $\lceil\frac{l}{5}\rceil-\lceil\frac{l}{10}\rceil$: $\partial P_5=Q_1\cdot Q_2$. As before, according to Lemma 4.8, the proportion of braids $x\in\mathcal{B}_n^{\varepsilon,l}$ such that Q_2 contains a blocking braid tends exponentially quickly to 1 (more precisely, according to [1], the number of braids for which this is not the case is of the order of $\lambda^{l-\frac{l}{10}}\mu^{\frac{l}{10}}$ for two constants $1<\mu<\lambda$, while the cardinality of $\mathcal{B}_n^{\varepsilon,l}$ is of the order of λ^l).

We now show the following: if x satisfies the condition of the lemma that P_1 is a prefix of ∂P_5, and if Q_2 contains a blocking braid, then the normal form of P_1 contains that of Q_1 as a prefix. For that, it suffices to prove that $\varphi(P_1^{-1}\partial P_5)\neq\varphi(\partial P_5)$ and to apply Lemma 4.6.

Let us recall that P_1 and ∂P_5 have the same length $\lceil\frac{l}{5}\rceil$. To simplify the notations, let us denote by $k=\lceil\frac{l}{5}\rceil$, and by $P_1=y_1\cdots y_k$ and $\partial P_5=z_1\cdots z_k$ the normal forms. The condition of the lemma is that $y_1\cdots y_k$ is a prefix of $z_1\cdots z_k$. Let us suppose for a contradiction that $\varphi(P_1^{-1}\partial P_5)=\varphi(\partial P_5)$, *i.e.* that $\varphi(y_l^{-1}\cdots y_1^{-1}z_1\cdots z_k)=z_k$. This means that

$$\mathrm{NF}_l(y_k^{-1}\cdots y_1^{-1}z_1\cdots z_k)=\mathrm{NF}_l(y_k^{-1}\cdots y_1^{-1}z_1\cdots z_{k-1})\cdot z_k$$

and in particular that $y_k^{-1}\cdots y_1^{-1}z_1\cdots z_{k-1}$ is a positive braid, *i.e.* that $y_1\cdots y_k$ is a prefix of $z_1\cdots z_{k-1}$. This is impossible, as $y_1\cdots y_k$ is a longer braid than $z_1\cdots z_{k-1}$.

We deduce that, if Q_2 contains a blocking braid, under the condition that P_1 is a prefix of ∂P_5, then the normal form of P_1 contains that of Q_1 as a prefix. A braid x satisfying these conditions is thus determined by at most $l-\lceil\frac{l}{10}\rceil$ factors, since the $\lceil\frac{l}{10}\rceil$ factors of Q_1 are determined by the first factors of P_1. So the proportion of such braids is, still according to [1], of the order of $\lambda^{-\frac{l}{10}}$.

Finally, among all braids of $\mathcal{B}_n^{\varepsilon,l}$, the proportion of elements such that P_1 is a prefix of ∂P_5 decreases exponentially quickly to 0 with l. This completes the proof of Lemma 4.9. □

Alternative proof of Lemma 4.9. We recall that P_1 and ∂P_5 have the same length $\lceil\frac{l}{5}\rceil$. To simplify the notations, we denote by $k=\lceil\frac{l}{5}\rceil$, and by $P_1=y_1\cdots y_k$ and $\partial P_5=z_1\cdots z_k$ the normal forms. Assume that $y_1\cdots y_k$ is a prefix of $z_1\cdots z_k$ – our aim is to show that this decreases substantially the number of possible words $y_1\cdots y_k$.

For $i=1,\dots,k-1$, the braid $y_1\cdots y_i$ should be a prefix of $z_1\cdots z_i$. Denote by δ_i the positive braid $y_i^{-1}\cdots y_1^{-1}z_1\cdots z_i$. As $y_{i+1}y_{i+2}\delta_{i+2}=\delta_i z_{i+1}z_{i+2}$, it follows that $y_{i+1}y_{i+2}$ is a divisor of

$\delta_i z_{i+1} z_{i+2}$; moreover, this last braid does not contain any Δ-factor (because if it did, then so would $\partial P_5 = y_1 \cdots y_i \delta_i z_{i+1} \cdots z_k$.) This enforces a strong restriction on the possible factors $y_{i+1} \cdot y_{i+2}$, beyond the obvious requirement that $y_i \cdot y_{i+1} \cdot y_{i+2}$ should be in normal form.

We will now use the fact (which we leave to the reader as an amusing exercise) that in every positive braid whose normal form contains exactly two factors, both different from Δ, there is a pair of strands that do not cross. In each divisor of such a braid the corresponding strands do not cross either. Let us apply this fact to the first two factors of $\delta_i z_{i+1} z_{i+2}$: there exists a pair of strands, the rth and the sth, that do not cross, and hence do not cross in $y_{i+1} y_{i+2}$, either. Let t be an element of $F(y_i)$. We can then construct a braid in normal form $y_{i+1} \cdot y_{i+2}$ such that $I(y_{i+1}) = \{t\}$ and where the rth and sth strands cross. (This is an easy exercise - for example, in $\mathcal{B}_6$ if $t = 1$, $r = 4$ and $s = 6$, we can choose $y_{i+1} \cdot y_{i+2} = \sigma_1\sigma_2\sigma_3 \cdot \sigma_3\sigma_4\sigma_5$; if $t = 3$, $r = 1$, $s = 6$, we choose $y_{i+1} \cdot y_{i+2}$ so that $y_{i+1} = \sigma_3\sigma_2\sigma_1\sigma_4\sigma_3\sigma_2\sigma_5\sigma_4\sigma_3$). This choice for y_{i+1} and y_{i+2} is therefore forbidden by the hypothesis that P_1 is a prefix of ∂P_5, even though $y_1 \cdots y_i \cdot y_{i+1} \cdot y_{i+2}$ is in normal form.

Since there is such a restriction for every value of i between 1 and $k-2$ (and this for every possible braid ∂P_5), the set of braids for which P_1 is a divisor of ∂P_5 has a lower rate of exponential growth than that of all braids. This implies Lemma 4.9. □

The proof of Proposition 3.4 is now complete. Let us summarize again: among the braids $x \in \mathcal{B}_n^{\epsilon,l}$, "generic" ones (a proportion which tends exponentially quickly to 1 as l tends to ∞) contain a blocking braid in their $P_2(x)$-segment (and, symmetrically, in $\partial P_4(x)$). For such a braid containing a blocking braid in P_2 and in ∂P_4, the only way to avoid being non-intrusively conjugate to a rigid braid is that, in the process of transforming $P_4P_5 \cdot P_1P_2$ into normal form

- either P_1 is completely absorbed into P_5, possibly creating some new factors Δ
- or, symmetrically, P_5 is completely absorbed into P_1.

As seen in Lemma 4.9, generically this does not happen (it only happens to a proportion of braids which tends exponentially quickly to 0). □

5. Pseudo-Anosov braids are generic

Theorem 5.1. *Consider the ball* $\mathbf{B}(l)$ *of radius* l *and center* 1 *in the Cayley graph of the braid group* $\mathcal{B}_n$*, with generators the simple braids. Then the proportion of pseudo-Anosov braids among the elements of this ball tends to 1 as* l *tends to infinity. Moreover, this convergence happens exponentially fast.*

Several key points of the proof come directly from [1].

Lemma 5.2. *There exists a constant* μ_{pA} *(which depends on* n*) such that, among the braids in* $\mathcal{B}_n^{\epsilon,l}$*, the proportion of those that can be non-intrusively conjugated to a rigid pseudo-Anosov braid is at least* $1 - \mu_{pA}^l$ *(for sufficiently large* l*, independently of* i*).*

Proof. Proposition 4.5 of the paper [1] explains how two theorems, one due to González-Meneses and Wiest, the other to Bernardete, Guttierez and Nitecki, can be used to prove that the normal form of a rigid braid which is not pseudo-Anosov satisfies some extremely restrictive conditions. More precisely, there are two words in normal form, one of length 2, the other of length 4, with the

following property: if the normal form of a rigid braid contains both of these words as subwords, then the braid is pseudo-Anosov.

Let us consider the proportion, among the elements x of $\mathcal{B}_n^{\epsilon,l}$, of braids which contain in their middle fifth $P_3(x)$ the two subwords mentioned in the previous paragraph. It follows from Lemma 4.8 that this proportion tends to 1 exponentially quickly: there exists a constant μ_M (which depends on n) such that this proportion is at least $1-\mu_M^l$. (The index M in the notation μ_M comes from the word "middle".)

We now look at the intersection of two subsets of $\mathcal{B}_n^{\epsilon,l}$:

(1) The braids in $\mathcal{B}_n^{\epsilon,l}$ which can be non-intrusively conjugated to a rigid braid
(2) The braids x in $\mathcal{B}_n^{\epsilon,l}$ which contain, in their middle fifth $P_3(x)$, the two subwords mentioned previously, which stop rigid braids from being reducible or periodic. (We insist that this second subset may well contain reducible braids, but none that are rigid *and* reducible.)

The braids belonging to this intersection are all pseudo-Anosov (in fact they are conjugate to rigid pseudo-Anosov braids). Moreover, for $l>0$, the proportion of elements of $\mathcal{B}_n^{\epsilon,l}$ which belong to the first subset is at least $1-\mu_R^l$ by Proposition 3.4, and for the second subset the proportion is bounded below by $1-\mu_M^l$. Hence the proportion of elements belonging to the intersection of the two is at least $1-\mu_R^l-\mu_M^l$. Thus for any μ_{pA} larger than $\max(\mu_R,\mu_M)$, we have the desired result. This concludes the proof of Lemma 5.2. □

Proof of Theorem 5.1. We are going to use three ingredients.

Firstly, we recall from [1] that there exists a number $\lambda>1$ (which depends on n) with the property that $|\mathcal{B}_n^{\epsilon,k}|=\Theta(\lambda^k)$, meaning that the sequences $\frac{|\mathcal{B}_n^{\epsilon,k}|}{\lambda^k}$ and $\frac{\lambda^k}{|\mathcal{B}_n^{\epsilon,k}|}$ stay bounded as k tends to infinity.

Secondly, as in [1] (Section 4.3), we observe that $\mathbf{B}(l)$, the ball of radius l and center 1 in the Cayley graph of $\mathcal{B}_n$, is the disjoint union

$$\mathbf{B}(l) \;=\; \bigcup_{k=0}^{l} \bigcup_{i=-l}^{l-k} \mathcal{B}_n^{\epsilon,k}$$

(This observation hinges on the fact that braids in so-called *mixed normal form* are geodesics, which is proven in [3].)

Thirdly, Lemma 5.2 ensures that among the elements of every $\mathcal{B}_n^{\epsilon,k}$, the proportion of braids not admitting a non-intrusive conjugation to a rigid pseudo-Anosov braid is an $O(\mu_{pA}^k)$, for a certain number μ_{pA} with $0<\mu_{pA}<1$.

The last two ingredients together imply that the total number of braids in $\mathbf{B}(l)$ which cannot be non-intrusively conjugated to a rigid pseudo-Anosov braid is a

$$O\left((2l+1)+2l\cdot(\lambda\cdot\mu_{pA})^1+(2l-1)\cdot(\lambda\cdot\mu_{pA})^2+\cdots+(2l-l+1)\cdot(\lambda\cdot\mu_{pA})^l\right)$$

Therefore, the proportion in $\mathbf{B}(l)$ of elements which cannot be non-intrusively conjugated to a rigid pseudo-Anosov braid is a

$$O\left(\frac{2l+1}{\lambda^l}+\frac{2l\cdot\mu_{pA}}{\lambda^{l-1}}+\frac{(2l-1)\cdot\mu_{pA}^2}{\lambda^{l-2}}+\ldots+\frac{(2l-l+1)\cdot\mu_{pA}^l}{1}\right)$$

$$\leqslant O\left((l+1)\cdot(2l+1)\cdot\left(\max(\tfrac{1}{\lambda},\mu_{pA})\right)^l\right)$$

and thus, for any $\varepsilon>0$, a

$$O\left(\left(\max(\tfrac{1}{\lambda},\mu_{pA})+\varepsilon\right)^l\right).$$

Choosing ε so small that $\max(\frac{1}{\lambda},\mu_{pA})+\varepsilon<1$ yields the result. □

6. Fast solutions to the conjugacy problem

The aim of this section is to prove that "generically, the conjugacy problem in B_n can be solved in quadratic time". First we recall a standard method for solving the conjugacy problem in braid groups. In order to decide whether two given braids x_1 and x_2 are conjugate, one calculates a certain finite subset $SC(x_i)$ of the conjugacy class of x_i, for $i=1,2$. We shall not need the precise definition of this subset, called the "sliding circuit set" $SC(x)$ of a braid x, we only need to know two things about it:

- The set $SC(x)$ depends only on the conjugacy class of x, and it is always non-empty.
- If the conjugacy class of x contains a rigid braid, then $SC(x)$ consists precisely of the rigid conjugates of x [7].

Now in order to decide whether x_1 and x_2 are conjugate, it suffices to test if an arbitrarily chosen element of $SC(x_1)$ is contained in $SC(x_2)$.

Our aim is to show that for a "generic" element x of $\mathcal{B}_n$, we can calculate the set $SC(x)$ in polynomial time.

Remark 6.1. We remark that for a rigid braid x_r, the set of rigid conjugates $SC(x_r)$ contains at least the orbit of x_r

- under τ, i.e. under conjugation by Δ, and
- under cyclic permutation of the factors other than Δ.

This orbit has at most $2\cdot\ell_c(x_r)$ elements. We will see later that for a "generic" braid, the set of rigid conjugates contains exactly *one* such orbit.

Theorem 6.2. *There exists an algorithm which takes as its input a braid $x\in\mathcal{B}_n$, whose running time is $O(\ell_c(x)^2)$, and which outputs*

(1) either a rigid conjugate of x, equipped with a certificate that the set of rigid conjugates of x contains only its orbit under the action of τ and under cyclic permutation of the factors (other than Δ),
(2) or the answer "I don't know".

Among the elements in the ball of radius l and center 1 in the Cayley graph of $\mathcal{B}_n$, the proportion of braids in case (2) tends to 0 exponentially fast as l tends to infinity.

Proof. As in section 4, we cut the braid x into 5 pieces P_1, P_2, P_3, P'_4 and P'_5, and we denote $P_4=\tau^{\inf x}(P'_4)$ and $P_5=\tau^{\inf x}(P'_5)$. We denote $P_{12}=P_1\cdot P_2$ and $P_{45}=P_4\cdot P_5$. (In fact, in order to describe the algorithmic procedure, it would be sufficient to cut the braid into only 3 pieces, but for explaining why the algorithm works it is more convenient to retain the notation of the previous sections.) Then we execute the following operations:

(1) calculate $\mathrm{NF}_l(P_{45}P_{12})$;
(2) test whether $\iota(P_{45}P_{12}) = \iota(P_{45})$. If this is false, answer "I don't know" and stop. If it is true, continue;
(3) test whether $\varphi(P_{45}P_{12}) = \varphi(P_{12})$. If this is false, answer "I don't know" and stop. If it is true, continue;
(4) test whether P_3 contains in its normal form the subword $(\Delta\sigma_2^{-1})\cdot\sigma_1$. If this is false, answer "I don't know" and stop. If it is true, continue;
(5) output $\Delta^{\inf x}P_{45}P_{12}P_3$.

Tests (2) and (3) check whether the conditions of Observation 4.2 hold for the braid x. If they do, then the braid $y = \Delta^{\inf x}P_{45}P_{12}P_3$ is indeed a rigid conjugate of x, and moreover there is a non-intrusive conjugation of x to y. Let us now suppose that x passes the test (4). Since the conjugation is non-intrusive, y also contains the subword $(\Delta\sigma_2^{-1})\cdot\sigma_1$. After a further cyclic permutation of the factors of y, we obtain a rigid braid z with $\iota(z) = \sigma_1$ and $\varphi(z) = (\Delta\sigma_2^{-1})$, or possibly $\iota(z) = \sigma_{n-1}$ and $\varphi(z) = \Delta\sigma_{n-2}^{-1}$.

We claim that under these circumstances the set $SC(z)$ consists only of the single orbit defined in Remark 6.1. The proof of this claim is essentially the same as the proof of Lemma 2.4 in[2]: it suffices to prove that conjugating z by any strict prefix of $\iota(z)$ or of $\partial\varphi(z)$ never yields an element of $SC(z)$. That, however, is a tautology: neither $\iota(z) = \sigma_1$ or σ_{n-1}, nor $\partial\varphi(z) = \sigma_2$ or σ_{n-2} have any strict prefixes!

This proves that the algorithm only gives the answers described in Theorem 6.2.

Let us now study the complexity of this algorithm. According to [6], calculating the normal form $\mathrm{NF}_l(P_{45}P_{12})$ has computational complexity $O(\ell_c(P_{45}P_{12})^2) = O(\ell_c(x)^2)$. The tests (2) and (3) are carried out in constant time, and test (4) in linear time. Thus the total complexity of the algorithm is indeed $O(\ell_c(x)^2)$.

Finally, we have to prove that the proportion of braids for which the algorithm answers "I don't know" tends to zero exponentially fast as l tends to infinity. This is a consequence of the properties shown in Section 4: the proportion of braids in the ball of radius l and center 1 in the Cayley graph satisfying the hypotheses of Observation 4.2 (i.e. tests (2) and (3)) goes to 1 exponentially quickly as l goes to infinity. According to Lemma 4.8, the same is true for the proportion of braids passing test (4). In summary, the proportion of braids failing one of the tests (2), (3), or (4), and thus generating an answer "I don't know", tends to zero exponentially quickly. □

Remark 6.3. In practice, test (4) should be replaced by "test whether P_3 contains in its normal form a subword of the form $(\Delta\sigma_j^{-1})\cdot\sigma_i$, $i \neq j$". This would not change the algorithm's $O(\ell_c(x)^2)$ complexity, and it would further increase the proportion of braids for which the algorithm outputs a rigid conjugate, rather than answering "I don't know".

7. Further consequences and questions

7.1. **Balls containing only pseudo-Anosov braids.**

Corollary 7.1. *For every positive integer l, there exists a vertex x in the Cayley graph of $\mathcal{B}_n$ such that the ball of radius l centered in x contains only pseudo-Anosov elements.*

Proof. Let us suppose, on the contrary, there is some number l such that the whole Cayley graph is covered by l-balls around non pseudo-Anosov elements. This would mean that together, the l-balls centered on the non pseudo-Anosov elements in $\mathbf{B}(R)$, the R-ball with center 1, cover the $(R-l)$-ball $\mathbf{B}(R-l)$, for arbitrarily large R. (Notice that they would not necessarily cover the whole R-ball $\mathbf{B}(R)$, because points that are l-close to its boundary might be covered by l-balls that are centered outside $\mathbf{B}(R)$.) We deduce that

$$\#(\beta \in \mathbf{B}(R), \beta \text{ non pseudo-Anosov}) \cdot \#(\mathbf{B}(l)) \geqslant \#(\mathbf{B}(R-l))$$

and therefore

$$\frac{\#(\beta \in \mathbf{B}(R), \beta \text{ non pseudo-Anosov})}{\#(\mathbf{B}(R))} \geqslant \frac{1}{\#(\mathbf{B}(l))} \cdot \frac{\#(\mathbf{B}(R-l))}{\#(\mathbf{B}(R))}.$$

When l is fixed and R tends to infinity, the right hand side remains bounded below by a positive number, because the braid group is of exponential growth. This is in contradiction with Theorem 5.1. □

We are grateful to Alessandro Sisto for pointing this corollary out to us. We have since learned from Saul Schleimer that this result was actually already known to certain specialists: it can also be proven by studying the action of $\mathcal{B}_n$ on Thurston's compactification of Teichmüller space.

7.2. **The closure of a generic braid is a hyperbolic link.**

Theorem 7.2. *Consider the ball* $\mathbf{B}(l)$ *of radius* l *and center* 1 *in the Cayley graph of the braid group* $\mathcal{B}_n$*, with generators the simple braids. Then, among the elements of this ball, the proportion of braids whose closure is a hyperbolic link tends to 1 as* l *tends to infinity.*

Proof. A theorem of T. Ito [9] states that a pseudo-Anosov braid x which in Dehornoy's total order of the braid group [5] does not satisfy $\Delta^{-4} < x < \Delta^4$, has the property that its closure is a hyperbolic link. Thus by our main theorem 5.1, it suffices to prove that, among the elements of $\mathbf{B}(l)$, the proportion of braids lying between Δ^{-4} and Δ^4 in Dehornoy's order tends to 0 as l tends to infinity.

In order to do so, we recall that if a braid x satisfies $\Delta^{j-1} < x < \Delta^j$, then Δx satisfies $\Delta^j < \Delta x < \Delta^{j+1}$. Now the l-ball in $\mathcal{B}_n$ is the disjoint union

$$\mathbf{B}(l) = \bigcup_{k=0}^{l} \bigcup_{x \in \mathcal{B}_n^{0,k}} \bigcup_{i=-l}^{l-k} \Delta^i x$$

We conclude with the observation that, among the $2l-k+1$ elements $\Delta^i x$, with $-l \leqslant i \leqslant l-k$, there are at most five lying between Δ^{-4} and Δ^4. □

7.3. **Questions.** It would be useful to extend our results to a much more general framework. From our proof, it is not even clear that Theorem 5.1 remains true if we replace Garside's generators with any other finite generating set, or if we replace $\mathcal{B}_n$ by a finite index subgroup (e.g. the pure braid group), or by its commutator subgroup, which is the kernel of the homomorphism $B_n \to \mathbb{Z}$ sending every Artin generator to 1.

For a start, one could try to adapt our arguments to the setting of general mapping class groups, equipped with Hamenstädt's bi-automatic structure [8].

We conjecture that the analogue, for our notion of "genericity", of the main result of Sisto [10] holds. Specifically, let G be a nonelementary group, equipped with a finite generating set and acting on a δ-hyperbolic complex, where at least one element of G acts weakly properly discontinuously (WPD). Then we conjecture that the proportion of elements in the l-ball of the Cayley graph of G with a WPD action tends to 1 exponentially quickly as l tends to infinity.

Acknowledgement We thanks François Digne and Juan González-Menses for many helpful and detailed comments on earlier versions of this article.

REFERENCES

[1] S. CARUSO, *On the genericity of pseudo-Anosov braids I: rigid braids*, `arXiv:1306.3757`
[2] S. CARUSO, *A family of pseudo-Anosov braids whose super summit sets grow exponentially*, to appear in J. Knot Theory Ram. 22 (2013), `arXiv:1302.5808`
[3] R. CHARNEY, J. MEIER, *The language of geodesics for Garside groups*, Math. Zeitschrift, 248 (2004), 495–509
[4] P. DEHORNOY, avec F. DIGNE, E. GODELLE, D. KRAMMER, J. MICHEL, *Foundations of Garside Theory*, book in preparation, preliminary version at `http://www.math.unicaen.fr/~garside/Garside.pdf`
[5] P. DEHORNOY, with I. DYNNIKOV, D. ROLFSEN, B. WIEST, *Ordering braids*, Providence, R.I.: American Mathematical Society, (2008).
[6] E. A. ELRIFAI, H. MORTON, *Algorithms for positive braids*, Q. J. Math., Oxf. II Ser., 45 (1994), p. 479 – 497
[7] V. GEBHARDT, J. GONZÁLEZ-MENESES, *The cyclic sliding operation in Garside groups*, Math. Z., 265 (2010), p. 85–114
[8] U. HAMENSTÄDT, *Geometry of the mapping class group II: A biautomatic structure*, arXiv:0912.0137
[9] T. ITO, *Braid ordering and the geometry of closed braid*, Geom. Topol. 15 (2011), p. 473–498
[10] A. SISTO, *Contracting elements and random walks* (2011), `arXiv:1112.2666`